REMARKS

Claims 1-38 are pending in this application. By this Amendment, the specification is amended to correct for typographical errors, Figures 7, 8, 13 and 20 are corrected to be consistent with the specification, and claims 1, 5, 7, 20, 21, 24, 25, 28, 31 and 33 are amended. No new matter is added. Reconsideration of the objections and rejections based on the above amendments and following remarks is respectfully requested.

The courtesies extended to Applicant's representative by Examiner Kim and Supervisory Patent Examiner Ayaz during the interview held March 30, 2004, are appreciated. The reasons presented at the interview as warranting favorable action are incorporated into the remarks below and constitute Applicant's record of the interview.

I. THE SPECIFICATION MEETS ALL FORMAL REQUIREMENTS

The Office Action objects to the specification because of an informality. The specification is amended based on an agreement with Examiners Kim and Ayaz during the March 30 personal interview. Withdrawal of the objection to the specification is respectfully requested.

II. THE DRAWINGS MEET ALL FORMAL REQUIREMENTS

The Office Action objects to the drawings for various informalities. The drawings are corrected based on an agreement with Examiners Kim and Ayaz during the March 30 personal interview. Withdrawal of the objection to the drawings is respectfully requested.

III. CLAIM 31 SATISFIES ALL FORMAL REQUIREMENTS

The Office Action, at page 3, erroneously indicates that claims 19 and 32 are objected. Based on an agreement with Examiners Kim and Ayaz during the March 30 personal interview, the Office Action should have indicated claim 31 as the objected claim.

Claim 31 is amended to obviate the objection, as discussed with, and agreed to, by Examiners Kim and Ayaz during the March 30 personal interview. Withdrawal of the objection to the claims is respectfully requested.

IV. CLAIMS 5, 7, 13, 20, 21, 24-26, 28 AND 33 SATISFY THE REQUIREMENTS OF 35 U.S.C. §112, SECOND PARAGRAPH

The Office Action rejects claims 5, 7, 24, 25, 28 and 33 under 35 U.S.C. §112, second paragraph, as being indefinite. Specifically, the Office Action asserts that the specification does not clearly define "means for creating a one-way function value X(M).

However, Examiners Kim and Ayaz agreed during the March 30 personal interview that the specification, at least at page 18, line 23 to page 19, line 25, and in Figs. 1 and 2, discloses a hash value calculation unit 5 that is used to create a one-way function value X(M).

Further, the Office Action rejects claims 7, 13, 20-21 and 24-26 under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements. Specifically, the Office Action asserts that the relationship between the one-way function X(M) and the private key X(M) is omitted.

Examiners Kim and Ayaz agreed during the March 30 personal interview that the specification, at least at page 21, lines 25-27, clearly discloses that "a private key processing unit 8 processes the hash value X(M) generated by the hash value calculation unit 5 as a private key." Thus, as set forth in claims 7, 20-21 and 24-26, a private key X(M) generated based on the hash value X(M), is further processed.

Accordingly, withdrawal of the rejections under 35 U.S.C. §112, second paragraph, is respectfully requested.

V. PENDING CLAIMS 1-38 DEFINE PATENTABLE SUBJECT MATTER

The Office Action rejects claims 1, 2, 5-10 and 19-20 under 35 U.S.C. §103(a) over U.S. Patent No. 6,154,541 to Zhang (hereinafter "Zhang") in view of U.S. Patent No.

6,240,513 to Friedman (hereinafter Friedman); claims 18, 21-30 and 33 under 35 U.S.C. §103(a) over Zhang in view of Friedman, and further in view of Stallings Cryptography and Network Security (hereinafter "Stallings"); claims 3, 4 and 11-17 under 35 U.S.C. §103(a) Zhang in view of Friedman, and further in view of Schneier Applied Cryptography (hereinafter "Schneider"); and claims 31, 32 and 34-38 under 35 U.S.C. §103(a) over Zhang in view of Friedman, Schneier and Stallings. The rejections are respectfully traversed.

As asserted by Applicant's representative during the March 30 personal interview, Zhang, alone or in combination with Friedman, Stallings or Schneier, fails to disclose or suggest a method for generating a one-way function dependent on a one-way function H and a unique value d, including *inter alia* holding a function generation unique value s **by a center**, creating a value generation unique value u from the function generation unique value s and the unique value d, **the value generation unique value u being provided to a user**, and creating a one-way function value X(M) of a message M by applying the one-way function H to the value generation unique value u and the message M, as set forth in independent claim 1, and similarly set forth in independent claims 5, 7, 20, 21, 24-26, 28 and 33. Support for the newly recited features is found in the original specification, at least at page 10, lines 5-18 and page 13, lines 6-16.

The Office Action, at page 5, admits that Zhang does not disclose holding a function generation unique value s. However, the Office Action asserts that this feature is known in the art. The Office Action further asserts that it would be obvious to one skilled in the art to store the unique value s locally, as taught by Friedman. Applicant respectfully disagrees with these assertions.

Friedman, at col. 5, lines 38-44, instead discloses that the seed s is held locally. In contrast to Friedman, claims 1, 5, 7, 20, 21, 24-26, 28 and 33 recite that the function generation unique value s is being held by a center.

Further, the Office Action, at page 5, admits that Zhang does not disclose creating a value generation unique value u from the function generation unique value s and the unique value d. However, the Office Action asserts that Zhang, at col. 21, line 65 to col. 22, line 36, teaches various "strategies of combining a plurality of parameters to generate new parameters." Thus, the Office Action asserts that it would have been obvious to use the strategies in Zhang to achieve the above feature. Applicant respectfully disagrees with this assertion.

As discussed above, neither Zhang nor Friedman discloses or suggests that the unique value s is being held by a center, as set forth in independent claims 1, 5, 7, 20, 21, 24-26, 28 and 33. Further, Zhang fails to disclose or suggest combining the function generation unique value s (which is held by the center) with the unique value d in order to create a value generation unique value u.

Because neither Schneier nor Stallings compensate for the deficiencies of Zhang and Friedman, Applicant respectfully submits that independent claims 1, 5, 7, 20, 21, 24-26, 28 and 33 are patentable over the applied art. Claims 2-4, 6, 8-19, 22, 23, 27, 29-32 and 34-38, which depend from claims 1, 5, 7, 21, 28 and 33 respectively, are also patentable over the applied art for at least the reasons discussed above. Accordingly, withdrawal of the rejections under 35 U.S.C. §103(a) is respectfully requested.

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable reconsideration and prompt allowance of claims 1-38 are earnestly solicited.

Should the Examiner believe that anything further would be desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number set forth below.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

George P. Simion
Registration No. 47,089

JAO:GPS/hs

Attachments:
Replacement Sheets, Figs. 7, 8, 13 and 20
Marked-up Replacement Sheets, Figs. 7, 8, 13 and 20

Date: May 13, 2004

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE
AUTHORIZATION
Please grant any extension
necessary for entry;
Charge any fee due to our
Deposit Account No. 15-0461